UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/682,526	09/14/2001	Aviel D. Rubin	2000-0415	3764

26652 7590 05/04/2005

AT&T CORP.
P.O. BOX 4110
MIDDLETOWN, NJ 07748

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/682,526	**Applicant(s)** RUBIN, AVIEL D.	
	Examiner Arezoo Sherkat	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 December 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 September 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

Response to Amendment

This office action is responsive to Applicant's remarks and amendment received on Dec. 2, 2004. Claims 5 and 13 have been amended. Claims 1-16 are pending.

Response to Arguments

Applicant's arguments see Remarks, Page 6, filed on 12/02/2004, with respect to claims 1-16 have been fully considered and are persuasive. The rejection of claims 1-16 has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of newly found prior art references.

The following is the new rejection:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bailey, III, (U.S. Patent No. 5,659,614 and Bailey hereinafter), in view of Cane et al., (U.S. Patent No. 5,940,507 and Cane hereinafter).

Regarding claims 1 and 9, Bailey discloses a method of backing up one or more files on a local device onto remote servers over a network comprising:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase (Col. 17-18, lines 1-67 and Col. 19, lines 1-5);

compressing one or more files and adding each of the files to a bundle, and encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server (Col. 17, lines 50-67 and Col. 18, lines 1-53).

Bailey does not expressly discloses generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle.

However, Cane discloses generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle (Col. 3, lines 55-67 and Col. 4, lines 1-37).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify Bailey's method and system for creating and storing a back up copy of file data stored on a computer by including the capability to generating an authentication code (i.e., CRC) for the bundle (i.e., message) using the first cryptographic key and adding the authentication code to the bundle as disclosed by Cane. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Cane to make it difficult to determine the original data without the proper key and ensure privacy and integrity of data upon retrieval (Cane, Col. 2, lines 10-35 and Abstract).

Regarding claims 5 and 13, Bailey discloses a method of restoring one or more files on remote servers to a local device over a network comprising:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase (Col. 17-18, lines 1-67 and Col. 19, lines 1-5);

decompressing one or more files from the bundle, and decrypting a bundle received from the remote server using the second cryptographic key (Col. 5, lines 7-33).

Bailey does not expressly disclose checking an authentication code in the bundle using the first cryptographic key.

However, Cane discloses checking an authentication code in the bundle using the first cryptographic key (Col. 3, lines 55-67 and Col. 4, lines 1-37).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify Bailey's method and system for creating and storing a back up copy of file data stored on a computer by including the capability to checking an authentication code in the bundle using the first cryptographic key as disclosed by Cane. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Cane to ensure privacy and integrity of data upon retrieval (Cane, Abstract).

Regarding claims 2, 6, 10, and 14, Bailey does not expressly disclose wherein the bundle is encrypted using a strong block cipher.

However, Cane discloses wherein the bundle is encrypted using a strong block cipher (Col. 3, lines 55-67 and Col. 4, lines 1-37).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify Bailey's method and system for creating and storing a back up copy of file data stored on a computer by including wherein the bundle is encrypted using a strong block cipher as disclosed by Cane. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Cane to ensure privacy and integrity of data upon retrieval (Cane, Abstract).

Regarding claims 4, 8, 12, and 16, Bailey does not expressly disclose wherein the cryptographic keys contain at least 128 bits.

However, Cane discloses wherein the cryptographic keys contain at least 128 bits (Col. 3, lines 55-67 and Col. 4, lines 1-37)(Note that MD2, MD4, and MD5 are message-digest algorithms. They are meant for digital signature applications where a large message has to be "compressed" in a secure manner before being signed with the private key. All three algorithms take a message of arbitrary length and produce a 128-bit message digest).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify Bailey's method and system for creating and storing a back up copy of file data stored on a computer by including wherein the cryptographic keys contain at least 128 bits as disclosed by Cane. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Cane to ensure privacy and integrity of data upon retrieval (Cane, Abstract).

Claims 3, 7, 11, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bailey, III, (U.S. Patent No. 5,659,614 and Bailey hereinafter) and Cane et al., (U.S. Patent No. 5,940,507 and Cane hereinafter), in view of Walmsley, (U.S. Publication No. 2004/0049468 and Walmsley hereinafter).

Regarding claims 3, 7, 11, and 15, Bailey or Cane does not expressly disclose wherein the authentication code is an HMAC.

However, Walmsley discloses wherein the authentication code is an HMAC (Pages 7-8, Par. 0157-0176).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the combined method and system of Bailey and Cane by including wherein the authentication code is an HMAC. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Walmsley to provide for a solution for Internet message authentication security protocols (Walmsley, Page 7, Par. 0158).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Linehan et al., (U.S. Patent No. 5,495,533),

Nozawa et al., (U.S. Patent No. 5,235,641), and

http://www.rsasecurity.com/rsalabs/node.asp?id=2253.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

A. Sherkat

Arezoo Sherkat
Patent Examiner
Group 2131
Apr. 26, 2005